Projet 3A

UF Informatique

Preuve formelle d'une runtime C haute intégrité

Introduction et contexte

AADL (*Architecture and Analysis Design Language*) [1] est un langage de description textuel et graphique d'architectures standardisé utilisé particulièrement dans le domaine aérospatial pour définir et concevoir des architectures avioniques. De nombreux outils permettent d'utiliser parmi lesquels :

- OSATE [2], une plateforme de modélisation développé par le Software Engineering Institute ;
- la chaîne TASTE [3] développée par l'ESA permettant de développer des systèmes embarqués temps-réel
- OCARINA [4], un outil de transformation de modèles pour AADL développé à l'ISAE.

En particulier, OCARINA permet de générer le code distribué Ada 2005 ou C99 correspondant à un modèle AADL donné et de l'exécuter ensuite sur une *runtime high-integrity*, PolyORB-HI (cf. [5] pour la *runtime* pour du code C).

Objectifs

L'objectif principal de ce projet est de prouver mathématiquement que la *runtime* PolyORB-HI/C est correcte fonctionnellement et qu'elle respecte des exigences de *safety* de base. Pour cela, les étudiants devront :

- comprendre le fonctionnement de PolyORB-HI/C sur un exemple simple et compléter sa documentation en utilisant Doxygen
- utiliser le langage de spécification formelle ACSL [6] pour spécifier chaque fonction de PolyORB-HI/C
- utiliser l'outil Frama-C [7] pour prouver formellement que le programme écrit en C respecte les spécifications écrites précédemment
- corriger les éventuelles erreurs détectées par les outils de preuve formelle

Une première étude a été faite l'an dernier et a permis de spécifier et de vérifier une partie de la *runtime* [8].

Encadrement

- Christophe Garion, ISAE/DMIA
- Jérôme Hugues, ISAE/DMIA

Références

[1] Carnegie Mellon University. *AADL*. 2013. URL : http://www.aadl.info/.

[2] CMU/SEI. *OSATE2*. 2013. URL : https://github.com/osate.

[3] European Space Agency. *taste – The Assert Set of Tools for Engineering*. 2013. URL : http://taste.tuxfamily.org/.

[4] ISAE et ESA. *Ocarina*. 2013. URL : http://www.openaadl.org.

[5] Telecom ParisTech. *PolyORB-HI C*. 2013. URL : http://penelope.enst.fr/aadl/wiki/PolyorbhicPresentation.

[6] Patrick Baudin et al. *ACSL : ANSI/ISO C Specication Language*. Version 1.7 – Fluorine-20130601. 2013. URL : http://frama-c.com/download/acsl-implementation-Fluorine-20130601.pdf.

[7] Patrick Baudin et al. *Frama-C*. 2012. URL : http://frama-c.com.

[8] Jérôme Hugues et Christophe Garion. *Formal verification of the PolyORB-HI/C middleware*. Technical report. ISAE, 2014.